Wprowadzenie

Rozwój Internetu zapoczątkował liczne zamiany ekonomiczno-społeczne i polityczne we współczesnym świecie. Stanowi również jedną z podstawowych przyczyn wzrostu zagrożenia cyberprzestępczością. Postęp techniczny wywiera przy tym bezpośredni wpływ na dynamikę przestępczości generowanej na tym obszarze. O ile tzw. pierwsza generacja cyberprzestępstw obejmowała głównie naruszenia integralności systemów komputerowych i modyfikację znajdujących się tam danych na skutek wprowadzenia programów określanych jako „wirus" lub „robak"[1], druga zaś była związana z rozwojem sieci teleinformatycznych[2] i atakami przez hackerów na bezpieczeństwo elektronicznie przetwarzanych w nich informacji[3], o tyle trzecia – obecna – jest związana z zauważalnym procesem „automatyzacji" cyberprzestępczości, będącej m.in. efektem wykorzystania złośliwego oprogramowania i botnetów. Trzecią generację cyberprzestępczości charakteryzuje przy tym: niskie prawdopodobieństwo wykrycia sprawcy oraz zorganizowane struktury przestępcze skupione wokół tzw. „podziemia

[1] Okres ten datuje się na lata 90. XX w. W tym okresie ataki przeprowadzane były głównie z wykorzystaniem wirusów i robaków komputerowych. Szczególnie charakterystyczne są ataki z wykorzystaniem Blastera, Czarnobyla, NetSky i Sassera, które zakłóciły pracę milionów komputerów na całym świecie. Dla cyberprzestępcy pierwszej generacji motywem przestępczego działania była zazwyczaj chęć uzyskania publicznego rozgłosu. *A. Završnik*, Cybercrime definitional challenges and criminological particularities, http://mujlt.law.muni.cz/storage/1236041878_sb_01-zavrsnik.pdf.

[2] System teleinformatyczny – według art. 2 pkt 3 ŚwiadUsłElektU – to „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. Nr 171, poz. 1800, z późn. zm.)". Grupa powiązanych ze sobą systemów teleinformatycznych jest rodzajem sieci telekomunikacyjnej, w której odbywa się przesyłanie i przetwarzanie danych, a jej powstanie związane jest z przenikaniem się rozległych sieci informatycznych i sieci telekomunikacyjnych. *X. Konarski*, Komentarz do ustawy o świadczeniu usług drogą elektroniczną, Warszawa 2004, s. 64. Zob. też *J. Piórkowska-Flieger*, [w:] Kodeks karny. Komentarz, *T. Bojarski* (red.), Warszawa 2012, s. 701.

[3] Na początku XXI w. cechą charakterystyczną drugiej generacji cyberprzestępczości jest działanie sprawców w celu osiągnięcia korzyści majątkowej. W tym celu wykorzystywane są botnety pozwalające rozsyłać miliony wiadomości spamowych, czy przeprowadzać ataki typu DoS. W tym czasie cyberprzestępcy zazwyczaj nie podejmowali działań zmierzających do ukrycia śladów swojej przestępczej działalności. *A. Završnik*, Cybercrime, http://mujlt.law.muni.cz/storage/1236041878_sb_01-zavrsnik.pdf.

komputerowego"[4]. Przestępcy komputerowi, obierając za cel konkretny system teleinformatyczny, używają kombinacji cichych i złożonych ataków z wykorzystaniem specjalnego oprogramowania (np. przy pomocy botów zbierają poufne informacje), przy pomocy *keyloggera* i *screen scrapera* uzyskują informację o nazwach użytkownika i hasłach dostępowych, czy też pozyskują poufne informacje wykorzystując w tym celu m.in. inżynierię społeczną (np. tworzą fałszywe strony internetowe)[5]. W odróżnieniu od pierwszej generacji cyberprzestępstw obecne ataki na systemy komputerowe nie są już tak chaotyczne i losowe (bazujące na wyszukiwaniu jakichkolwiek podatnych lub błędnie zabezpieczonych systemów), ale bardziej profesjonalne i ukierunkowane na konkretny cel (np. serwer, system komputerowy, usługę, firmę). Zmasowane cyberataki na instytucje odpowiedzialne za obronę narodową i bezpieczeństwo przestrzeni powietrznej, czy ogólnie na struktury krytyczne państwa nie tylko przestały być wizją z gatunku *science-fiction*, ale także domeną hackera wykorzystującego jedynie własne umiejętności.

Rozmiar i tendencje cyberprzestępczości stanowią realny sprawdzian dla obowiązującego prawa karnego. Skuteczne przeciwdziałanie temu zjawisku wymaga w pierwszej kolejności, ze względu na zasadę podwójnej karalności oraz internacjonalny charakter Internetu, przyjęcia jednolitych rozwiązań prawnych w ustawodawstwie karnym jak największej liczby państw. Brak takich rozwiązań połączony z różnorodnością norm międzynarodowego prawa karnego[6], ustano-

[4] W niektórych opracowaniach wyróżnia się również czwartą generację cyberprzestępczości, charakteryzującą się coraz powszechniejszym wykorzystywaniem przez sprawcę narzędzi hackerskich oraz dalszym rozwojem podziemia komputerowego. Zob. np.: http://i.dell.com/sites/doccontent/business/smb/sb360/en/Documents/wp-swx-cybercrime-generation.pdf. Zob. też na temat funkcjonowania podziemia komputerowego i czarnego rynku z nim związanego np. Panda Security, 2010. The Cybercrime Black Market: Uncovered, http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf.

[5] Według raportu na temat cyberprzestępczości z lutego 2013 r. przygotowanego przez Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości (United Nations Office on Drugs and Crime) ponad 80% cyberataków pochodzi od zorganizowanych grup przestępczych i jest związane z działaniem tzw. podziemia komputerowego odpowiedzialnego m.in. za tworzenie szkodliwego oprogramowania, zarządzanie botnetami, pozyskiwanie poufnych danych osobowych i finansowych. Raport analizuje ustawodawstwo 97 państw członkowskich ONZ, spośród których 56 państw odpowiedziało na przygotowaną przez biuro ankietę. Raport dostępny online na: http://www.unodc.org/documents/commissions/CCPCJ_session22/13-80699_Ebook_2013_study_CRP5.pdf.

[6] W piśmiennictwie zauważalny jest brak spójności poglądów w kwestii rozumienia pojęcia „międzynarodowe prawo karne". Przyjmując najszersze znaczenie, obejmuje ono wszelkie aspekty międzynarodowej odpowiedzialności karnej. Chodzi więc o „[...] gałąź prawa zawierającą normy prawa międzynarodowego publicznego, kształtujące bezpośrednio lub pośrednio zakres penalizacji, zasady odpowiedzialności karnej i postępowania karnego, a także normy prawa międzynarodowego i wewnętrznego odnoszące się do przestępstw z elementem obcym lub do instytucji współpracy międzynarodowej w sprawach karnych". *L. Gardocki*, O pojęciu prawa karnego międzynarodowego,

wionych przez poszczególne państwa może np. prowadzić do wielu praktycznych problemów związanych z możliwością pociągnięcia do odpowiedzialności karnej osób uważanych za przestępców w części państw o bardziej restrykcyjnych regulacjach normatywnych, zaś z drugiej strony chronionych przez inne, z racji przyznania im większej ochrony. Dodatkowo konieczne wydaje się istotne zaangażowanie europejskich służb policyjnych i specjalnych w celu przeciwdziałania zagrożeniom powodowanym przez cyberprzestępców. Oczywiste pozostaje przy tym, że praktykę policyjną i śledczą intensywnie musi wspomagać kryminalistyczna teoria wykrywania, która określa logicznie powiązane działania prowadzące od ofiary czy wydarzenia do sprawcy. Niejednokrotnie wyrafinowany *modus operandi* sprawcy[7], brak dokładnej definicji zjawiska i zagadnień szczegółowych, a także mechanizmów zwalczania, poważnie utrudnia nie tylko rozpoznanie i wykrywanie, ale również zgromadzenie dowodów przestępstwa. We wszystkim tym nie pomaga niejednoznaczność przepisów prawnych, a skuteczne zwalczanie tego zjawiska rozwijającego się nie tylko ilościowo, ale również jakościowo wydaje się niemożliwe bez ciągłego dostosowywania zarówno metod przeciwdziałania, jak i obowiązującego prawa. Wskazaną potrzebę uzasadnia w szczególności pojawianie się nowych form zagrożeń cyberprzestępczości związanych z jej profesjonalizacją i uzawodowieniem struktur przestępnych.

Wychodząc naprzeciw wskazanym powyżej potrzebom niniejsze opracowanie zostało poświęcone zrekonstruowaniu międzynarodowych standardów normatywnych kryminalizacji cyberprzestępstw oraz wstępnej charakterystyce analizowanych zachowań przestępnych. Posłużyć to ma nie tylko celom czysto poznawczym, co przede wszystkim opracowaniu instrumentalnie skutecznej strategii przeciwdziałania (zapobiegania i ścigania).

Przedmiotem niniejszego opracowania jest również ocena polskiego ustawodawstwa karnego materialnego w aspekcie dostosowania zawartych w nim rozwiązań do postanowień podpisanej w dniu 23.11.2001 r. w Bukareszcie

---

PiP 1984, z. 3, s. 79–80. Zob. też *M. Królikowski*, *P. Wiliński*, *J. Izydorczyk*, Podstawy prawa karnego międzynarodowego, Warszawa 2008; *M. Płachta*, Status i pojęcie międzynarodowego prawa karnego, Prok. i Pr. 2009, Nr 5, s. 5–16; *R. Sonnenfeld*, Pojęcie „międzynarodowego prawa karnego publicznego", PiP 1984, z. 3, s. 62–70; *T. Srogosz*, Wokół sporów o przedmiocie „prawa karnego międzynarodowego", Gubernaculum et Administratio 2002, Nr 2, s. 157–163; *J. Waszczyński*, Czy międzynarodowe prawo karne stanowi samodzielną dziedzinę prawa? Acta UŁ Fol.Iur. 1985, Nr 22, s. 53–63.

[7] W najbardziej ogólnym znaczeniu *modus operandi* to sposób działania sprawcy i zacierania śladów popełnionego czynu. Zdaniem *T. Hanauska*, „to taki, charakterystyczny i z reguły powtarzalny sposób zachowania się sprawcy, który stanowiąc odbicie jego najczęściej indywidualnych cech, właściwości i możliwości, wyraża się swoiście w czynie przestępnym, następstwach czynu, a szczególnie w śladach, niekiedy także i w zachowaniach poprzedzających czyn lub następujących po nim, lecz w ścisłym z nim związku". *T. Hanausek*, *Modus operandi* i alibi – ewolucja znaczenia pojęć, SKKiP 1978, t. 8, s. 221, tam szersza literatura.

pod auspicjami Rady Europy, Konwencji o cyberprzestępczości (ETS/STE No. 185)[8], która jest obecnie na szczeblu międzynarodowym uznawana za najbardziej kompletny zbiór norm międzynarodowych w zakresie ścigania cyberprzestępstw oraz do prawa unijnego, w tym w szczególności do Decyzji ramowej 2005/222/WSiSW w sprawie ataków na systemy informatyczne (Dz.Urz. UE L 69 z 16.3.2005 r.) i Dyrektywy Parlamentu Europejskiego i Rady 2011/92/UE z 13.12.2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L 335/1 z 17.12.2011 r.). Wobec dostrzegalnej konieczności ciągłego przystosowywania wielu instytucji prawnych do zmieniającego się środowiska sieci i systemów komputerowych celem niniejszej pracy będzie także ocena, czy propagowane we wskazanych powyżej dokumentach międzynarodowych standardy normatywne są rozwiązaniem optymalnym i skutecznym dla osiągnięcia stawianych przed nimi celów.

Ocena zakresu i sposobu kryminalizacji cyberprzestępstw na gruncie polskiego ustawodawstwa dokonana zostanie także z uwzględnieniem wypracowanych na gruncie prawa karnego wybranych państw–stron Konwencji Rady Europy instrumentów prawnych, służących do walki z cyberprzestępczością oraz wybranych dokumentów międzynarodowych, w tym w szczególności: Prawa Modelowego Wspólnot Narodów, dotyczącego przestępstw komputerowych i przestępstw związanych z komputerami (*Commonwealth Model Law on Computer and Computer Related Crime* – LMM(02)17[9]) oraz przygotowanego pod auspicjami ONZ przez Międzynarodowy Związek Telekomunikacyjny opracowania pt. *ITU Cybercrime Legislation Toolkit*[10]. Szeroki wgląd w międzynarodowe standardy normatywne kryminalizacji cyberprzestępstw, a także w sposoby ich zwalczania ma od strony metodologicznej swoje szersze uzasadnienie z uwagi na wyraźną internacjonalizację tej przestępczości. Ponadto, przy powszechnie zauważalnej integracji gospodarczej i politycznej Europy, automa-

[8] Na listę cyberprzestępstw, przewidzianych w Konwencji, składają się: a) przestępstwa przeciwko poufności, integralności i dostępności danych komputerowych i systemów obejmujące: nielegalny dostęp (art. 2), nielegalne przechwytywanie danych (art. 3), naruszenie integralności danych (art. 4), naruszenie integralności systemu (art. 5), niewłaściwe użycie urządzeń (art. 6), b) przestępstwa komputerowe obejmujące: fałszerstwo komputerowe (art. 7), oszustwo komputerowe (art. 8), c) przestępstwa ze względu na charakter zawartych informacji: przestępstwa związane z pornografią dziecięcą (art. 9) d) przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych (art. 10 Konwencji RE).

[9] Dalej jako Prawo Modelowe Wspólnot Narodów. Tekst dokumentu dostępny na: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

[10] Tekst dokumentu dostępny na: http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf.

tyzacji działania sieci i systemów teleinformatycznych oraz dynamicznym rozwoju transgranicznych usług świadczonych drogą elektroniczną konieczne wydaje się nie tylko dostosowywanie wewnętrznego prawa karnego do porządku prawnego Rady Europy, jak i Unii Europejskiej[11], ale również otwarcia na modelowe rozwiązania zagraniczne warte recepcji i upowszechnienia[12].

Właściwa analiza i rozpoznanie prezentowanej problematyki wymagała zastosowania kilku metod badawczych. Poza podstawową dla prac prawniczych metodą analizy formalno-dogmatycznej, w najszerszym zakresie skorzystano z metody prawnoporównawczej. Odniesienie się do orzeczeń sądowych zapadłych, zarówno przed krajowymi oraz zagranicznymi sądami, jak i do krajowych oraz obcojęzycznych opracowań teoretycznych, pozwoliło na praktyczne zastosowanie dokonanej analizy, wskazanie możliwych w tej płaszczyźnie rozwiązań i dróg rozwoju, a także na zweryfikowanie słuszności i skuteczności koncepcji proponowanych w prawie krajowym, nie tracąc z pola widzenia imperatywu zapewnienia skutecznej harmonizacji prawa.

Analiza zagadnień stanowiących przedmiot niniejszego opracowania, na wzór podziału cyberprzestępstw przyjętego w Konwencji RE o cyberprzestępczości, dzieli się na trzy rozdziały poświęcone odpowiednio:

1) przestępstwom przeciwko poufności, integralności i dostępności danych i systemów komputerowych (tzw. przestępstwa *stricte* komputerowe),
2) przestępstwom związanym z użyciem środków masowego przekazu do rozpowszechniania lub prezentowania informacji zakazanych przez prawo (tzw. przestępstwa związane z treścią informacji),
3) przestępstwom instrumentalnego wykorzystania (użycia) elektronicznych sieci informatycznych i systemów teleinformatycznych do naruszania dóbr prawnych chronionych przez prawo karne (przestępstwa związane z użyciem komputera i sieci teleinformatycznych), w tym także przestępstwom przeciwko mieniu związanym z naruszeniem praw autorskich i praw pokrewnych.

Punktem wyjścia do wskazanej problematyki jest kryminologiczna analiza uwzględniająca statystyczno-empiryczne aspekty analizy zjawiska cyberprzestępczości, czemu poświęcony został Rozdział I pracy. Wyniki referowanych w tej części badań posłużą zarówno przedstawieniu natury cyberprzestępczości,

[11] Należy nadmienić, że zapewnienie skuteczności umowie międzynarodowej w krajowym porządku prawnym wymaga także wykładni zgodnej z jej założeniami.

[12] Przy całym zauważalnym wzroście znaczenia „międzypaństwowego prawa karnego" należy wyrazić ogólny sceptycyzm co do możliwości dokonania takiej unifikacji prawa, której ostatecznym rezultatem byłby jeden europejski kodeks karny. Por. *M. Cieślak*, W kwestii międzynarodowej unifikacji prawa karnego, ZNWPiAUG 1978, z. 7, s. 71; *A. Adamski*, Uwagi na temat harmonizacji prawa karnego materialnego w Unii Europejskiej, [w:] Przestępstwo – kara – polityka kryminalna. Problemy tworzenia i funkcjonowania prawa, Kraków 2006, s. 23 i n. Zob. też *M. Siwicki*, Podstawy określenia jurysdykcji w sprawach cyberprzestępstw w UE, EPS 2013, Nr 9, s. 20–26.

jak i problemów metodologicznych pojawiających się przy oszacowaniu rzeczywistych rozmiarów tego zjawiska. Ten rozdział opracowania przedstawia również międzynarodowe inicjatywy w zakresie przeciwdziałania i karalności cyberprzestępczości. Rozważania nad ww. elementami stanowią wprowadzenie do analizy zagadnień mających znaczenie praktyczne: poznanie sposobów i środków działania cyberprzestępców, ustalenie obszarów zagrożonych działalnością tych sprawców oraz wskazanie na wybrane zagadnienia związane z zapobieganiem cyberprzestępczości.

Zagadnienia szczegółowe wchodzące w zakres kolejnych trzech rozdziałów w założeniu mają odpowiadać następującej strukturze:

1) przedstawieniu międzynarodowych standardów kryminalizacji wybranego przestępstwa,
2) analizie ustawodawstwa polskiego w przedmiotowym zakresie,
3) ocenie polskiego ustawodawstwa i sformułowaniu wniosków *de lege lata* oraz *de lege ferenda* w przypadkach potrzeby nowelizacji ustawodawstwa polskiego.

W opracowaniu świadomie zrezygnowano ze formułowania oddzielnych wniosków na końcu pracy. Postulaty te są prezentowane na bieżąco w toku rozważań, co w załażeniu ma ułatwić ich krytyczną ocenę.

W Rozdziale II, przed analizą poszczególnych modeli ochrony bezpieczeństwa elektronicznie przetwarzanej informacji i próbą oceny polskiego ustawodawstwa karnego materialnego, niezbędne okazało się wyjaśnienie wielu pojęć z zakresu informatyki, w tym w szczególności takich jak: „dane i programy komputerowe", „system informatyczny", czy też „sieć i system komputerowy". Bezkrytyczne i bezwarunkowe odwoływanie się do zastanych konwencji terminologicznych i intuicji, a także brak dobrej znajomości technicznego wymiaru przestępstw *stricte* komputerowych prowadzić może bowiem nie tylko do wielu nieporozumień, ale znacznie szkodzi każdej analizie dogmatycznej. Należy przy tym zauważyć, że akty prawne, zarówno w Polsce, jak i w Europie, posługują się w tym zakresie bardzo zróżnicowaną terminologią i często nie do końca precyzyjną. Poza wskazanym wymiarem dogmatycznym, podniesiona problematyka terminologiczna ma również aspekt bardziej pragmatyczny związany z dążeniem do uzyskania jednoznacznego opisu całego typu przestępstwa.

W Rozdziale III odnoszącym się do przestępstw związanych z treścią informacji, w części poświęconej przestępstwom przeciwko wolności seksualnej na szkodę małoletniego omówiono dodatkowo nowo wprowadzony do ustawy karnej czyn w postaci zakazanego nawiązywania kontaktu z małoletnim za pośrednictwem systemu teleinformatycznego i sieci telekomunikacyjnej, będący wyrazem dostosowywania prawa polskiego do Konwencji Rady Europy z Lanzarote o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych (*Council of Europe Convention on the Protection of*

Children against Sexual Exploitation and Sexual Abuse – CETS No. 201), podpisanej przez Polskę 25.10.2007 r. Wskazany rozdział zawiera również analizę dogmatyczną przepisów prawnych związanych z ochroną czci (zniewaga, zniesławienie) w warunkach instrumentalnego wykorzystania przez sprawcę szeroko pojętej techniki komputerowej.

Rozdział IV, oprócz analizy zakresu kryminalizacji przestępstw związanych z użyciem komputera i sieci informatycznych na tle Konwencji RE o cyberprzestępczości i Decyzji ramowej w sprawie ataków na systemy informatyczne (oszustwo komputerowe i fałszerstwo komputerowe), poświęcony został również szczególnie groźnemu zjawisku „kradzieży tożsamości" oraz „cyberstalkingu".

Katalog przestępstw, które mogą być popełnione przy użyciu nowoczesnych technologii jest zdecydowanie szerszy niż wskazany w niniejszym opracowaniu. Celem niniejszej pracy nie jest jednak analiza wszystkich czynów zabronionych określanych mianem cyberprzestępstwa, lecz próba oceny kilku z nich, mających najbardziej istotne znaczenie praktyczne.

Ze względu na ograniczone ramy niniejszej książki pominięto problematykę przeciwdziałania cyberterroryzmowi[13]. Niniejsze opracowanie nie odnosi się również do problematyki kryminalizacji zachowań motywowanych rasizmem, faszyzmem i ksenofobią. Temu zagadnieniu poświęcona została jednak wydana przez autora w 2011 r. monografia pt. „Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne", która zawiera szeroką analizę polskiego ustawodawstwa karnego na tle prawnoporównawczym, w tym także na tle Konwencji Rady Europy o cyberprzestępczości wraz z protokołem dodatkowym, dotyczącym penalizacji czynów o charakterze rasistowskim i ksenofobicz-

[13] Termin „cyberterroryzm" ogólnie służy do określenia grupy czynów, polegających na posługiwaniu się elektronicznymi systemami przetwarzania informacji w działalności terrorystycznej. Ograniczeniem formalnym jest wymóg karalności w wymiarze, co najmniej 5 lat pozbawienia wolności (art. 115 § 20 KK), co powoduje, że jedynie przestępstwa z art. 165 § 1 pkt 4 i art. 269 § 1 KK będą mogły być zakwalifikowane do przestępstw o charakterze terrorystycznym. Większość przestępstw skierowanych przeciwko informacjom, danym i systemom je przetwarzającym, *de facto* mogących posiadać przymiot terroryzmu, nie będzie mogła być uznana i ścigana jako terrorystyczne. Zagadnieniu cyberterroryzmu poświęcono uwagę m.in., w: *M. Madej*, *A. Bógdał-Brzezińska*, *M. F. Gawrycki*, Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003; *S. Serwiak*, Cyberterroryzm – nowe zagrożenie dla bezpieczeństwa, Arch.Krymin. 2005/2006, Nr 28, s. 345–365; *R. Łuksiewicz*, Rozwój informatyczny a cyberterroryzm, [w:] Wojna z terroryzmem w XXI wieku, *B. Hołyst*, *K. Jałoszyński*, *A. Letkiewicz* (red.), Szczytno 2009, s. 109–122; *A. Suchorzewska*, Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem, Warszawa 2010; *J. W. Wócik*, Przeciwdziałanie przestępczości zorganizowanej. Zagadnienia prawne, kryminologiczne i kryminalistyczne, Warszawa 2011; *tenże*, Cyberterroryzm nowe wyzwania XXI wieku, Prok. i Pr. 2010, Nr 3, s. 161–171; *tenże*, Przeciwdziałanie finansowaniu terroryzmu, Warszawa 2007; *A. Adamski*, Cyberterroryzm, [w:] Terroryzm. Materiały z sesji naukowej (Toruń 11.4.2001 r.), *V. Kwiatkowska-Darul* (red.), Toruń 2002, s. 113–121.

nym popełnionych przy użyciu systemów komputerowych oraz Decyzji ramowej Rady 2008/913/WSiSW z 28.11.2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych (Dz.Urz. UE L 328 z 6.12.2008 r., s. 55–58). Pominięte zostały także aspekty procesowe ścigania omawianych przestępstw oraz związane z tym zagadaniem problemy prawne i kryminalistyczne, w szczególności w zakresie gromadzenia dowodów winy sprawców czynów zabronionych. Istniejące bariery techniczne i prawne w postępowaniu dowodowym niewątpliwie należą do podstawowych czynników warunkujących niewielką wykrywalność sprawców cyberprzestępstw i tłumaczą powściągliwość organów procesowych wobec ścigania przestępstw popełnianych przy użyciu nowoczesnych technologii przetwarzania informacji. Są to jednak problemy ogólne, którym w literaturze poświęca się coraz więcej uwagi[14].

[14] Zagadnieniem procesu karnego oraz procesowych instrumentów ścigania przestępstw popełnionych przy pomocy nowoczesnych technologii przetwarzania informacji (w tym Internetu) zajmują się np.: *A. Adamski*, Prawo, s. 183–217; *B. Fisher*, Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne, Kraków 2000; *P. Królikowski*, Zarys problematyki dowodu elektronicznego oraz jego zabezpieczania z punktu widzenia techniki i taktyki kryminalistycznej, [w:] Problemy współczesnej kryminalistyki, t. 13, *E. Gruza*, *T. Tomaszewski*, *M. Goc* (red.), Warszawa 2009, s. 71–97; *A. Lach*, Dowody elektroniczne w procesie karnym, Toruń 2004; *tenże*, Dowody elektroniczne w sprawach pornografii dziecięcej i pedofilii w Internecie, [w:] Internet. Ochrona wolności, własności i bezpieczeństwa, *G. Szpor* (red.), Warszawa 2011, s. 419–426; *tenże*, Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego, Prok. i Pr. 2003, Nr 10, s. 16–25; *tenże*, Dowody cyfrowe w postępowaniu karnym – wybrane zagadnienia praktyczne i teoretyczne, MoP 2005, Nr 3 (dodatek Prawo Mediów Elektronicznych Nr 2), s. 43–46; *G. Nauka*, Prawnicza informatyka korporacyjna. Dowody elektroniczne w postępowaniu karnym, Prok. i Pr. 2008, Nr 7/8, s. 250–255; *P. Wiliński*, Korzystanie z dowodów elektronicznych w procesie karnym, [w:] Prawo wobec wyzwań współczesności, t. 4. Materiały sesji naukowej (Poznań 15.2.2006 r.), *P. Wiliński*, *O. Krajniak*, *B. Guzik* (red.), Poznań 2007, s. 215–220.

Rozdział I. Cyberprzestępczość – charakterystyka zjawiska

Na początku lat 90. XX w. dostęp do Internetu posiadało około 3 miliony osób, z czego 73% pochodziło z USA, zaś 15% z Europy Zachodniej. Pozostała część użytkowników zamieszkiwała w Kanadzie, Australii, Japonii, Republice Korei i Izraelu. W tym okresie, poza wskazanymi państwami, dostęp do Internetu był prawie niemożliwy[1]. Dziesięć lat później szacowano, że liczba użytkowników Internetu wzrosła do prawie 369 milionów osób. W 2010 r. – po upływie kolejnej dekady – szacuje się, że na świecie jest prawie dwa miliardy użytkowników Internetu, pięć miliardów telefonów komórkowych, 255 milionów stron internetowych, zaś dziennie wysyła się ponad 294 milionów wiadomości e-mail oraz 5 miliardów SMS-ów[2].

Obecnie społeczeństwo w znacznym stopniu uzależnione jest od niezakłóconego funkcjonowania nowoczesnych technologii informacyjnych. Komputery wykorzystywane są m.in. do kontroli i zarządzania przedsiębiorstwami, wspomagania lotnictwa, dostaw energii, wody, czy świadczenia różnego rodzaju usług telekomunikacyjnych. Wszystko to sprawia, że nadużycia komputerowe stają się coraz powszechniejszym zagrożeniem nie tylko dla bezpieczeństwa narodowego, krytycznych infrastruktur krajowych (takich jak przedsiębiorstwa wodociągowe czy zaopatrzenie w energię), sektora finansowego (w szczególności banków), biznesu (szpiegostwo, ujawnienie tajemnicy przedsiębiorstwa), ale całych społeczności.

§ 1. Pojęcie i kategoryzacja cyberprzestępstw

I. Problematyka terminologiczna

W latach 60. XX w. wraz z rozwojem nowych technologii i ich wykorzystywaniem w celach przestępnych pojawiała się potrzeba określenia grupy czynów, polegających na posługiwaniu się komputerem do naruszania dóbr prawnych

[1] Dokładne statystki dostępne na http://www.worldmapper.org/display.php?selected=335.
[2] Zob. http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/.

tradycyjnie chronionych przez prawo karne. W literaturze przedmiotu, opisując to zjawisko, zaczęto posługiwać się takimi pojęciami jak „przestępczość komputerowa" lub „przestępstwa związane z wykorzystaniem komputera"[3]. Od początku pojawienia się tych terminów wskazywano na liczne wątpliwości, co do ich zakresu znaczeniowego.

Początkowo termin przestępczość komputerowa był rozumiany dwojako. Po pierwsze, jako przestępstwa komputerowe określano grupę czynów, polegających na posługiwaniu się komputerem do naruszenia jakiegokolwiek dobra prawnego chronionego przez prawo karne[4]. W tym ujęciu komputer stanowił przedmiot lub środowisko zamachu. Po drugie, termin ten służył dla określenia przestępstw, które były popełniane przez osoby o wysokich umiejętnościach i wiedzy z zakresu elektroniki lub informatyki. W tym drugim ujęciu posiadanie przez sprawcę szczególnej wiedzy i umiejętności było traktowane jako istotny element przestępczości komputerowej. Z tego też względu pojawiały się propozycje używania określenia przestępczość informatyczna (ang. *crime in information science*, franc. *la criminalite informatique*) wyraźnie odwołując się do dyscypliny naukowej zajmującej się m.in. technologiami przetwarzania informacji oraz technologiami wytwarzania systemów przetwarzających informacje[5].

Zarówno kryminolodzy, jaki i dogmatycy prawa karnego podjęli się wielu prób ścisłego zdefiniowania i nazwania przestępstw popełnianych z wykorzystaniem nowoczesnej technologii komputerowej[6]. Na przykład w Niemczech, które są jednym z pionierów innowacyjnych rozwiązań legislacyjnych z zakresu prawa

---

[3] *A. Adamski*, Prawo, s. 30.

[4] Legalnej definicji „pojęcia komputer" na próżno poszukiwać można na gruncie prawa europejskiego. Nie oznacza to jednak, że żaden ze współczesnych ustawodawców nie podjął się próby stworzenia ogólnej definicji prawnej tego pojęcia. Definicję komputera zawiera ustawodawstwo amerykańskie. Według 18 USC § 1030(e)(1) komputer to: „elektroniczne, magnetyczne, optyczne, elektrochemiczne lub inne urządzenie służące do szybkiej transmisji danych wykonujące funkcje logiczne, arytmetyczne lub funkcję przechowywania". Pojęcie komputer obejmuje również „wszelkie obiekty przeznaczone do przechowywania danych lub komunikacji bezpośrednio związane lub współdziałające z takimi urządzeniami". Jednocześnie za komputer nie uznaje się „automatycznej maszyny do pisania lub składu drukarskiego, przenośnego kalkulatora, czy też innego podobnego urządzenia". Podstawową zaletą takiego rozwiązania jest jednoznaczne określenie statusu prawnego niektórych urządzeń. Z drugiej strony, jego mankamentem jest brak elastyczności szczególnie wskazany do w stosunku do urządzeń, które podlegają tak dynamicznym zmianom. Według wskazanej definicji za komputer uznać można na przykład telefon komórkowy, jak i odtwarzacz mp3, czy nawet sprzęt gospodarstwa domowego, w tym m.in. niektóre lodówki, czy odtwarzacze DVD. Powyższe problemy ilustruje sprawa *USA v. Mitra* [405 F 3d 492 (7th Cir 2005), dostępne na: http://www.leagle.com/decision/2005897405F3d492_1843], w której za komputer uznano system radiowy używany przez policję, ponieważ był on wyposażony w „procesor umożliwiający szybkie przetwarzanie danych" oraz krótkofalówki, ze względu na ich bezpośrednie współdziałanie z centralą.

[5] *A. Završnik*, Cybercrime, http://mujlt.law.muni.cz/storage/1236041878_sb_01-zavrsnik.pdf.

[6] Zob. *M. Siwicki*, Podział i definicja cyberprzestępstw, Prok. i Pr. 2012, Nr 7–8, s. 246–256.